



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,536	08/03/2001	John R. McGarvey	5577-236	6803

20792 7590 08/18/2006

MYERS BIGEL SIBLEY & SAJOVEC  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER
----------

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 08/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 09/921,536	Applicant(s) MCGARVEY ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 02 March 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2131

1 This action is in response to the communication filed on 3/2/2006.

2 ***Response to Arguments***

3 Applicant's arguments filed 3/2/2006 have been fully considered but they are not  
4 persuasive.

5 Regarding applicants' argument that Brezak and Ganesan did not disclose "a common  
6 nonce *associated with each of the plurality of servers*" the examiner does not find the argument  
7 persuasive. The PAC of Brezak is associated with each of the servers 212-216 in that the PAC is  
8 provided to server 210 in order to authenticate the client 202 to the servers 212-216. This can be  
9 seen in Brezak Paragraph 0043, which disclosed the client sending an service ticket in a request  
10 AP\_REQ to server A, Paragraph 0045, which disclosed that the service ticket was forwarded to  
11 the authentication service by server A, and Paragraphs 0049-0052, which disclosed that the PAC  
12 was included with the service ticket, and that the PAC held information regarding access  
13 restriction for the client, and Paragraphs 0045-0048, which disclosed that the client was  
14 authenticated based on the service ticket, and Paragraph 0052 further shows that the access  
15 restriction information of the PAC was used in selectively allowing access to certain  
16 servers/services. As such, because the PAC is involved in controlling access to the servers, it is  
17 associated with the servers. Therefore, the examiner does not find the argument persuasive.

18 Regarding applicants' argument regarding claim 2, the argument has been considered but  
19 is moot in view of the new grounds of rejection presented and necessitated by the amendment to  
20 claim 2.

21

22

Art Unit: 2131

**DETAILED ACTION**

All objections and rejections not set forth below have been withdrawn.

Claims 1-32 have been examined.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

Claims 1, 23-29, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brezak et al. (US Patent Application Publication 2003/0018913) hereinafter referred to as Brezak, and further in view of Ganesan (US Patent Number 5,535,276).

Regarding claim 1, Brezak disclosed a method for a middle tier server to impersonate a client to a plurality of servers, the method comprising: obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043 and Paragraph 0049 "PAC"); providing the common nonce to the client (See Brezak Fig. 2 Paragraph 0043 Lines 3-6); receiving the common nonce at the middle tier server (See Brezak Paragraph 0043 Lines 6-9), and providing the common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers (See Brezak Paragraph 0044, Paragraph 0055 Lines 12-14, and Paragraph 0057 Lines 3-7).

Art Unit: 2131

1           However, Brezak failed to disclose the client signing the common nonce (PAC).

2           Ganesan teaches that in a ticketing system, in order to protect against dictionary attacks,  
3   the ticket should be encrypted by the ticket granting system with the key shared between the  
4   server to be accessed and the ticket granting server (See Ganesan Col. 5 Lines 34-56), and the  
5   user should sign the ticket (TEMP-CERT) (See Ganesan Col. 15 Lines 45-60).

6           It would have been obvious to the ordinary person skilled in the art at the time of  
7   invention to employ the teachings of Ganesan in the ticketing system of Brezak by having the  
8   ticket encrypted with server/ticket granting system keys, and having the client sign the service  
9   ticket before sending the ticket to the Server A. This would have been obvious because the  
10   ordinary person skilled in the art would have been motivated to provide protection against  
11   dictionary attacks against the ticket.

12          Regarding claim 26, the combination of Brezak and Ganesan disclosed a system for a  
13   middle tier server to impersonate a client to a plurality of servers, the system comprising: means  
14   for obtaining a common nonce associated with each of the plurality of servers from an entity  
15   other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043 and  
16   Paragraph 0049 "PAC"); means for providing the common nonce to the client (See Brezak Fig. 2  
17   Paragraph 0043 Lines 3-6)); means for receiving the common nonce signed by the client at the  
18   middle tier server (See Brezak Paragraph 0043 Lines 6-9 and Ganesan Col. 15 Lines 45-60), and  
19   means for providing the common nonce to the plurality of servers as a signature for transactions  
20   so as to authenticate the client to the plurality of servers (See Brezak Paragraph 0044 and  
21   Paragraph 0055 Lines 12-14 and Paragraph 0057 Lines 3-7).

Art Unit: 2131

1        Regarding claim 27, the combination of Brezak and Ganesan disclosed a computer  
2        program product (See Brezak Paragraph 0015) for a middle tier server to impersonate a client to  
3        a plurality of servers, comprising: a computer readable media having computer readable program  
4        code embodied therein, the computer readable program code comprising: computer readable  
5        program code that obtains a common nonce associated with each of the plurality of servers from  
6        an entity other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043  
7        and Paragraph 49 "PAC"); computer readable program code that provides the common nonce to  
8        the client (See Brezak Fig. 2 Paragraph 0043 Lines 3-6)); computer readable program code that  
9        receives the common nonce signed by the client at the middle tier server (See Brezak Paragraph  
10       0043 Lines 6-9 and Ganesan Col. 15 Lines 45-60), and computer readable program code that  
11       provides the common nonce to the plurality of servers as a signature for transactions so as to  
12       authenticate the client to the plurality of servers (See Brezak Paragraph 0044 and Paragraph 0055  
13       Lines 12-14 and Paragraph 0057 Lines 3-7).

14       Regarding claim 28, the combination of Brezak and Ganesan disclosed a method of  
15       authenticating a client, comprising: receiving at a server of a plurality of servers, a common  
16       nonce that is provided to each of the plurality of servers from an entity other than the client of  
17       the plurality of servers (See Brezak Paragraphs 0048-0049 and 0057), the common nonce being  
18       signed by the client (See Ganesan Col. 15 Lines 45-60), and authenticating the client based on  
19       the received signed common nonce (See Brezak Paragraphs 0048-0049 and 0057).

20       Regarding claim 31, the combination of Brezak and Ganesan disclosed a system for  
21       authenticating a client, comprising: means for receiving at a server of a plurality of servers, a  
22       common nonce that is provided to each of the plurality of servers from an entity other than the

1 client of the plurality of servers (See Brezak Paragraphs 0048-0049 and 0057), the common  
2 nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and means for  
3 authenticating the client based on the received signed common nonce (See Brezak Paragraphs  
4 0048-0049 and 0057).

5       Regarding claim 32, the combination of Brezak and Ganesan disclosed a computer  
6 program product for authenticating a client, comprising: a computer readable media having  
7 computer readable program code embodied therein (See Brezak Paragraph 0015), the computer  
8 readable program code comprising: computer readable program code which receiving at a server  
9 of a plurality of servers, a common nonce that is provided to each of the plurality of servers from  
10 an entity other than the client of the plurality of servers (See Brezak Paragraphs 0048-0049 and  
11 0057), the common nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and  
12 computer readable program code which authenticates the client based on the received signed  
13 common nonce (See Brezak Paragraphs 0048-0049 and 0057).

14  
15       Regarding claim 23, the combination of Brezak and Ganesan disclosed that the step of  
16 obtaining a common nonce comprises the steps of: obtaining the common nonce from a party  
17 trusted by the middle-tier server and the plurality of servers, the common nonce being signed by  
18 the trusted party; and verifying the signature of the common nonce is the signature of the trusted  
19 party (See the rejection of claim 1 above, especially Ganesan Col. 5 Lines 34-56).

20       Regarding claim 24, the combination of Brezak and Ganesan disclosed that at least one of  
21 the plurality of servers carries out the steps of: receiving a client certificate, determining if the

Art Unit: 2131

1 client certificate is trusted; and indicating that the client is not authenticated if the client  
2 certificate is not trusted (See Brezak Paragraph 0055).

3 Regarding claim 25, the combination of Brezak and Ganesan disclosed that at least one of  
4 the plurality of servers carries out the steps of: receiving the signed common nonce and a client  
5 certificate; determining if the signature of the signed common nonce corresponds to a signature  
6 of the client certificate; and indicating that the client is not authenticated if the signature of the  
7 signed common nonce does not correspond to the signature of the client certificate (See Ganesan  
8 Col. 16 Line 64 – Col. 17 Line 5 and Col. 17 Lines 56-61).

9 Regarding claim 29, the combination of Brezak and Ganesan disclosed that the common  
10 nonce is provided by a trusted third party (See Brezak Paragraph 43).

11  
12 Claims 2-3, 5, 7-11, 14-15, and 30 are rejected under 35 U.S.C. 103(a) as being  
13 unpatentable over the combination of Brezak and Ganesan as applied to claim 2 above, and  
14 further in view of Ford (US Patent Number 6,829,356).

15 Regarding claims 2-3, and 30, Brezak and Ganesan disclosed a Trusted Third Party  
16 generating the common nonce based on information of the plurality of servers (See the rejection  
17 of claim 1 above), but failed to disclose obtaining pre-nonce contributions from the plurality of  
18 servers; combining the pre-nonce contributions to provide a single pre-nonce token; and  
19 providing the common nonce based on the pre-nonce token.

20 Ford teaches a system in which a client can authenticate to a plurality of servers by  
21 signing proof data generated from a plurality of nonces associated with a plurality of servers (See  
22 Ford Col. 15 Line 9 – Col. 16 Line 14) involving obtaining pre-nonce contributions from the



1 plurality of servers (See Ford Col. 15 Lines 24-31); combining the pre-nonce contributions to  
2 provide a single pre-nonce token; and providing the common nonce based on the pre-nonce  
3 token (See Ford Col. 15 Lines 56-61).

4 It would have been obvious to the ordinary person skilled in the art at the time of  
5 invention to employ the teachings of Ford in the ticketing and authentication system of Brezak  
6 and Ganesan by providing the ticket granter with server nonces, combining the nonces, and  
7 placing the nonces in the ticket to be signed. This would have been obvious because the ordinary  
8 person skilled in the art would have been motivated to provide strong secret data which could be  
9 verified in the ticket.

10 Regarding claim 5, the combination of Brezak, Ganesan, and Ford disclosed that the step  
11 of combining the pre-nonce contributions to provide a single pre-nonce token comprises  
12 concatenating the pre-nonce contributions (See Ford Col. 15 Lines 56-61).

13 Regarding claim 7, the combination of Brezak, Ganesan, and Ford disclosed that the step  
14 of obtaining pre-nonce contributions comprises the steps of: requesting a pre-nonce contribution  
15 from each of the plurality of servers (See Ford Col. 15 Paragraph 2); and receiving the pre-nonce  
16 contributions from the plurality of servers (See Ford Col. 15 Paragraph 2).

17 Regarding claim 8, the combination of Brezak, Ganesan, and Ford disclosed that  
18 requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of  
19 servers (See Ford Col. 15 Lines 1-22).

20 Regarding claim 9, the combination of Brezak, Ganesan, and Ford disclosed the step of  
21 encrypting the authenticated requests sent to the plurality of servers (See Ford Col. 15 Paragraph  
22 1).

Art Unit: 2131

1           Regarding claim 10, the combination of Brezak, Ganesan, and Ford disclosed that the  
2           authenticated requests include at least one of an identification of a source of the request, a time  
3           stamp and a random number (See Brezak Paragraph 0051).

4           Regarding claim 11, the combination of Brezak, Ganesan, and Ford disclosed that the  
5           pre-nonce contributions include at least one of an identification of a server of the plurality of  
6           servers and a random number (See Ford Col. 15 Lines 24-38, and Line 56 Col. 16 Line 2).

7           Regarding claim 14, the combination of Brezak, Ganesan, and Ford disclosed the steps  
8           of: receiving a transaction identification from a trusted server of the plurality of servers; and  
9           associating the transaction identification with the common nonce (See Ford Col. 15 Lines 22-  
10          31).

11          Regarding claim 15, the combination of Brezak, Ganesan, and Ford disclosed the step of  
12          tracking use of the common nonce based on the transaction identification (See Ford Col. 15 Line  
13          22 - Col. 16 Line 2).

14          Claims 4, 6, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
15          the combination of Brezak, Ganesan, and Ford as applied to claim 3 above, and further in view  
16          of Schneier (Applied Cryptography).

17          Regarding claim 4, the combination of Ford and Blakley disclosed providing a common  
18          nonce (See Ford Col. 15 Lines 56-61), but failed to disclose reducing the nonce challenges to  
19          provide the common nonce. However, Ford and Blakley did disclose digitally signing a message  
20          containing the nonce challenges (See Ford Col. 15 Lines 56-61).

21          Schneier teaches that when digitally signing a message, it is practical to hash the message  
22          and encrypt the hash, with a private key, as the signature, rather than encrypting the whole

1 message (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and  
2 One-Way Hash Functions). Schneier also teaches that in such a system, to verify the signature,  
3 the verifier hashes the message, decrypts the signed hash with the signers public key, and verifies  
4 that the two hashes are the same (See Schneier Page 38 Section Signing Documents with Public-  
5 Key Cryptography and One-Way Hash Functions).

6 It would have been obvious to the ordinary person skilled in the art at the time of  
7 invention to employ the teachings of Schneier in the digital signatures of Brezak, Ganesan, and  
8 Ford by signing and verifying the hash of the nonce message instead of the whole nonce  
9 message. This would have been obvious because the ordinary person skilled in the art would  
10 have been motivated to increase the speed of the signing method.

11 Regarding claim 6, the combination of Brezak, Ganesan, Ford, and Schneier disclosed  
12 that the step of reducing the pre-nonce token to provide the common nonce comprises the step of  
13 hashing the pre-nonce token utilizing a one-way hash function so as to provide the common  
14 nonce (See the rejection of claim 4 above).

15 Regarding claim 20, the combination of Brezak, Ganesan, Ford, and Schneier disclosed  
16 that at least one of the plurality of servers carries out the steps of: receiving the signed common  
17 nonce, the common nonce and the pre-nonce token; hashing the received pre-nonce token;  
18 comparing the hashed pre-nonce token to the common nonce; indicating that the client is not  
19 authenticated if the hashed pre-nonce token is different from the common nonce (See Ford Col.  
20 15 Lines 56-65 and Schneier Page 38 Section Signing Documents with Public-Key Cryptography  
21 and One-Way Hash Functions).

1           Regarding claims 12-13, the combination of Brezak, Ganesan, and Ford disclosed the  
2   client checking the nonce challenge from the server for requisite strength, and aborting the  
3   authentication process if the nonce challenge did not meet the requisite strength (See Ford Col.  
4   15 Lines 39-41), but failed to disclose that this check included checking the signature of the  
5   nonce challenge to verify that it was signed by the server.

6           Schneier teaches that digital signatures provide a means for verifying the sender of a  
7   message (See Schneier Page 37 Signing Documents with Public Key Cryptography).

8   It would have been obvious to the ordinary person skilled in the art at the time of invention to  
9   employ the teachings of Schneier in the nonce challenge system of Ford and Blakley by having  
10   the server sign the challenges and having the client verify the signature of the challenges before  
11   using the challenges. This would have been obvious because the ordinary person skilled in the  
12   art would have been motivated to protect against illicit alteration of the challenge nonce.

13          Claims 16-19, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
14   the combination of Brezak, Ganesan, and Ford as applied to claim 3 above, and further in view  
15   of Menezes et al. (Handbook of Applied Cryptography).

16          The combination of Brezak, Ganesan, and Ford disclosed the server receiving the nonce  
17   challenges, and authenticating the client based on whether the nonce challenges included the  
18   nonce challenge of the server (See Ford Col. 15 Lines 56-65), but failed to disclose that the  
19   nonce challenges included random numbers. The combination further disclosed using a users  
20   public key to verify the signature of the nonce message by verifying that the signature  
21   corresponded to the signature of the clients private/public key pair (See Ford Col. 15 Lines 56-

Art Unit: 2131

65), but failed to disclose that the verifying server got the public key from a public key certificate and also failed to disclose that the authentication would fail if the certificate was not trusted.

Menezes teaches that nonce challenges can be random numbers (See Menezes Page 398).

Menezes further teaches that when using nonce challenges the challenger should apply a timeout

period to the nonce and not authenticate the client if the response is received after the timeout

period has expired (See Menezes Page 398 Section (i)). Menezes teaches further still that public

key certificates are a means to store, distribute, and forward public keys without danger of

undetectable manipulation. Menezes also teaches that when using a certificate for

authentication, the certificate is received, the expiration date is checked, the certification

authority validity is checked, the signature of the certificate is checked, and the certificate is

checked to see if it has been revoked, and if these checks pass then the public key is valid (See

Menezes Pages 559-560).

It would have been obvious to the ordinary person skilled in the art at the time of

invention to employ the teachings of Menezes in the nonce challenge system of Brezak,

Ganesan, and Ford by having the nonce challenges be random numbers and by applying and

checking a timeout period to the nonce when authenticating a client. This would have been

obvious because the ordinary person skilled in the art would have been motivated to provide

uniqueness and timeliness assurances in the system in order to avoid replay and interleaving

attacks. It further would have been obvious to employ the teachings of Menezes in the

authentication system of Brezak, Ganesan and Ford by obtaining the public key from a public

key certificate and verifying that the certificate is valid in order to use the public key to

1 authenticate the client. This would have been obvious because the ordinary person skilled in the  
2 art would have been motivated to protect against undetected manipulation of the public key.

3 ***Conclusion***

4 Claims 1-32 have been rejected.

5 Applicant's amendment necessitated the new ground(s) of rejection presented in this  
6 Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

7 Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


8 A shortened statutory period for reply to this final action is set to expire **THREE**  
9 **MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**  
10 **MONTHS** of the mailing date of this final action and the advisory action is not mailed until after  
11 the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period  
12 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37  
13 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,  
14 however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this  
15 final action.

16  
17 Any inquiry concerning this communication or earlier communications from the  
18 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.  
19 The examiner can normally be reached on M-F 8-4.

20 If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
21 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
22 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent  
2 Application Information Retrieval (PAIR) system. Status information for published applications  
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished  
4 applications is available through Private PAIR only. For more information about the PAIR  
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR  
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would  
7 like assistance from a USPTO Customer Service Representative or access to the automated  
8 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9  
10  
11  
12  
13  
14   
15 Matthew Henning  
16 Assistant Examiner  
17 Art Unit 2131  
8/16/2006

CHRISTOPHER REVAK  
PRIMARY EXAMINER

 8/16/06